

Attestation in TLS

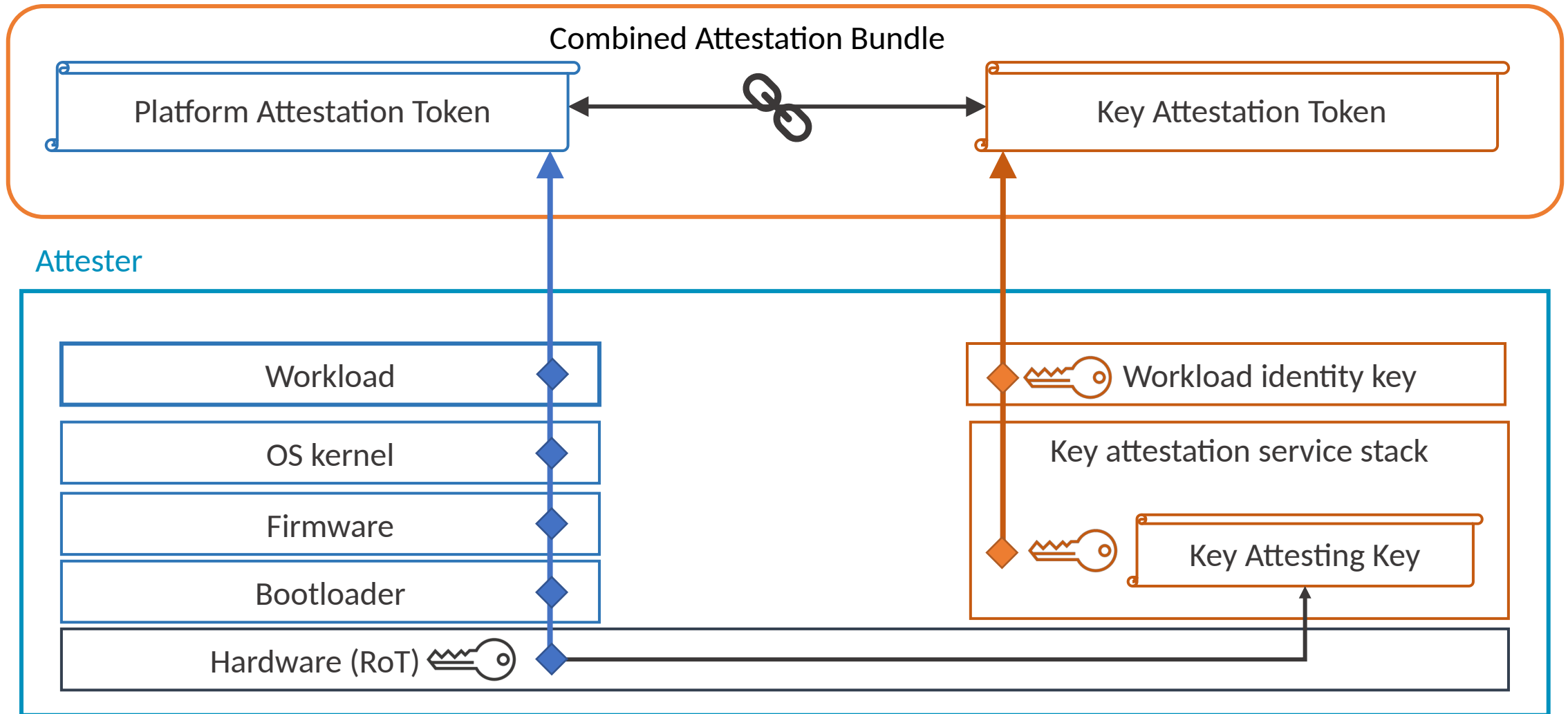
Introduction

- Historically Transport Layer Security (TLS) protocol has relied on Public Key Infrastructure (PKI) for authentication
- Remote Attestation presents an enhancement to PKI, leveraging hardware features to provide comprehensive information about the security state of the device
- Our work is focused on standardising remote attestation as a native authentication mechanism in TLS
- Also backed by an Open-Source proof of concept project, backed by Confidential Consortium Attestation Special Interest Group

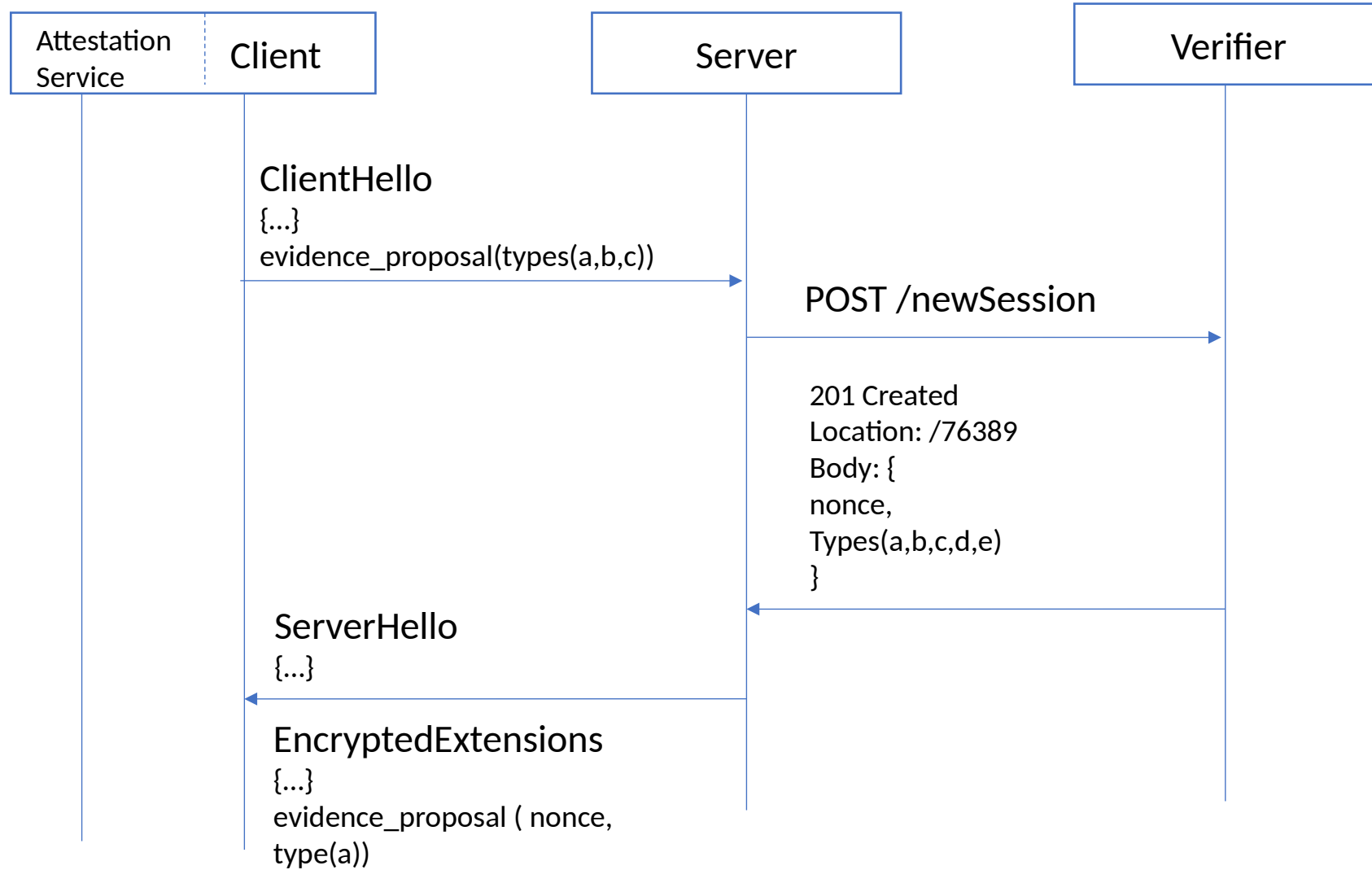
TLS Extensions

- We're defining a new certificate type
- Attestation metadata is carried instead of (or together with) an X.509 certificate
- Attestation metadata itself is opaque to the TLS implementation
- Also defining new TLS extensions that allow negotiation of the credential type, and conveyance of freshness
- Authenticating both Client and Server

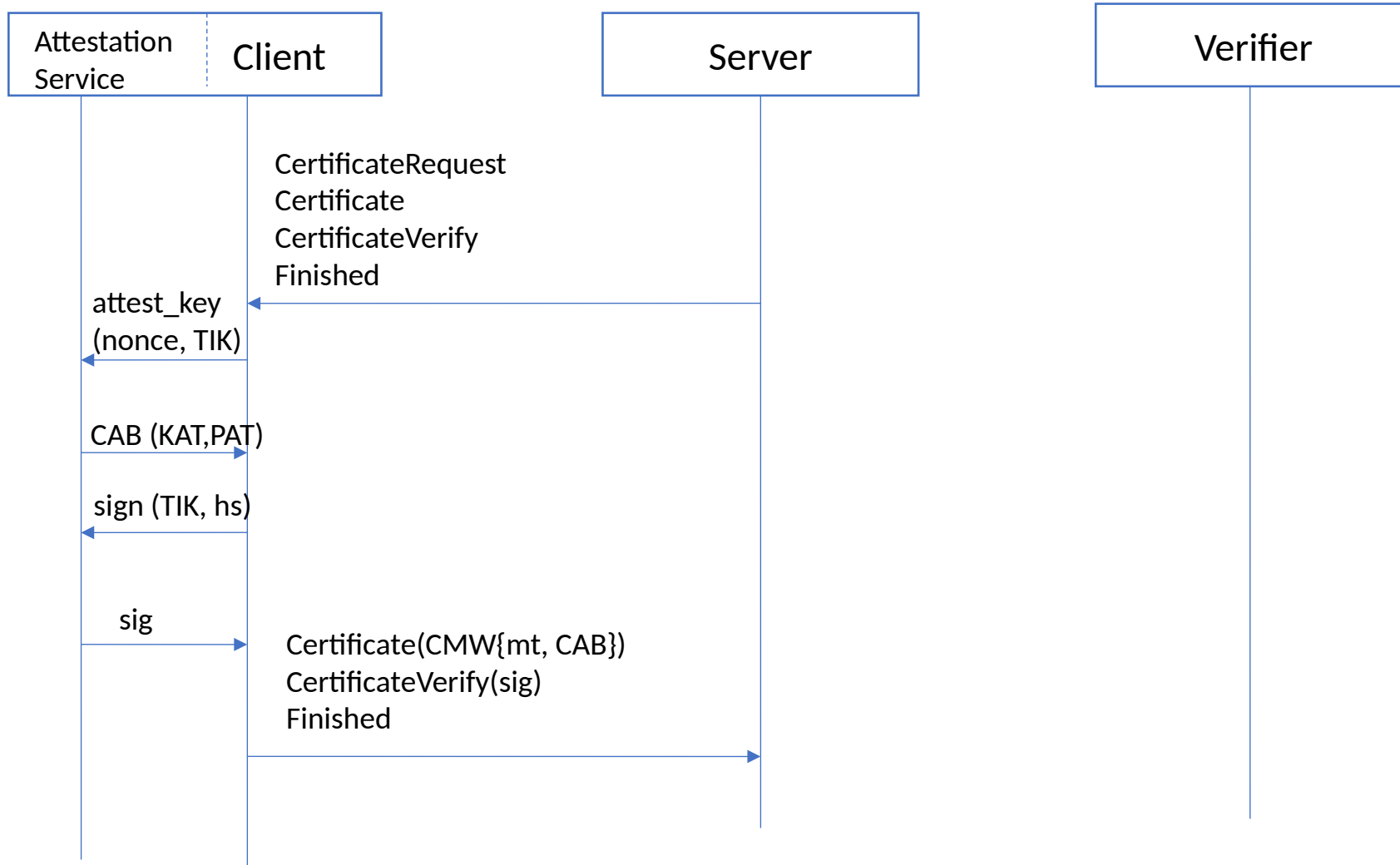
Key & Platform attestation



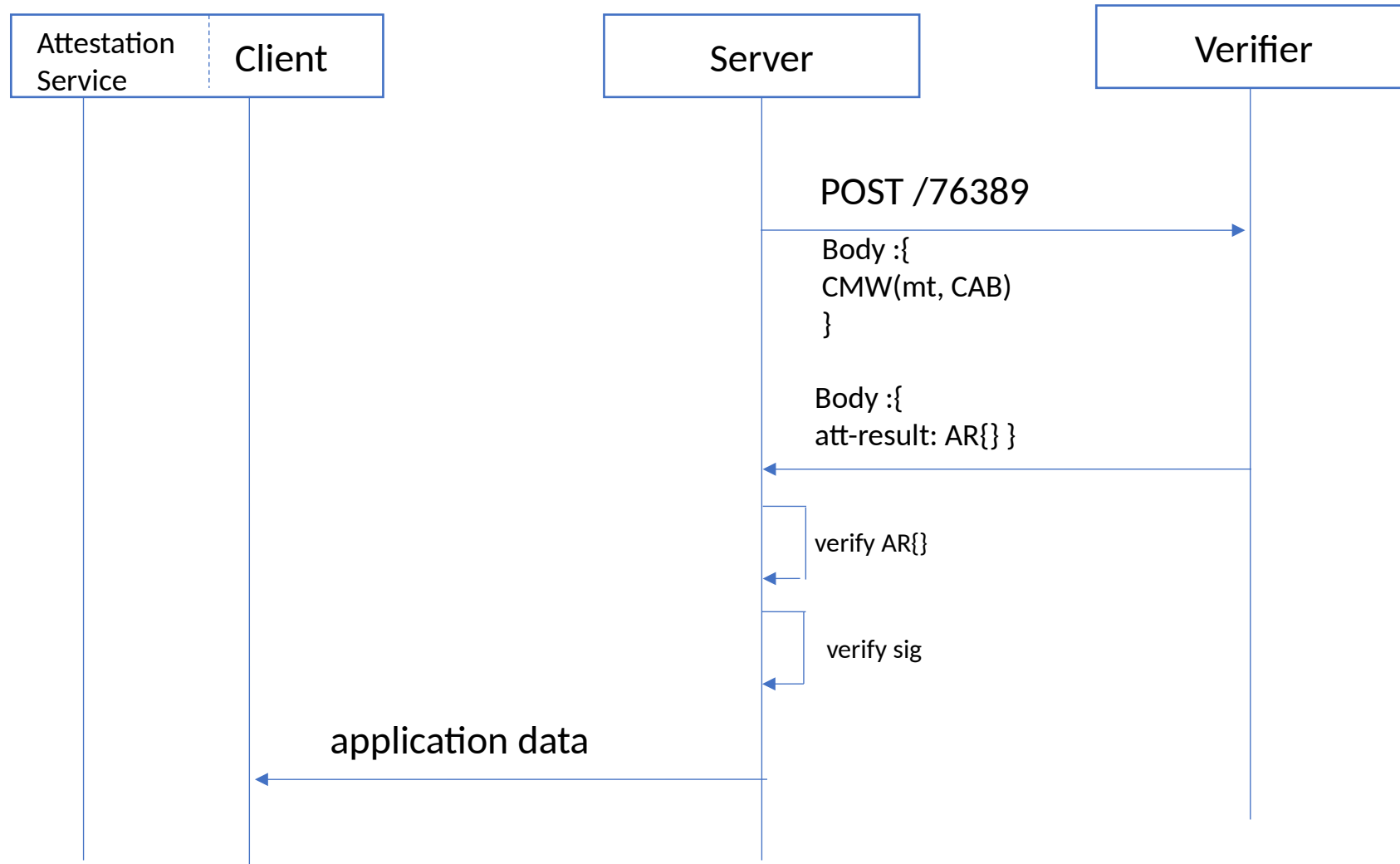
Message Flow



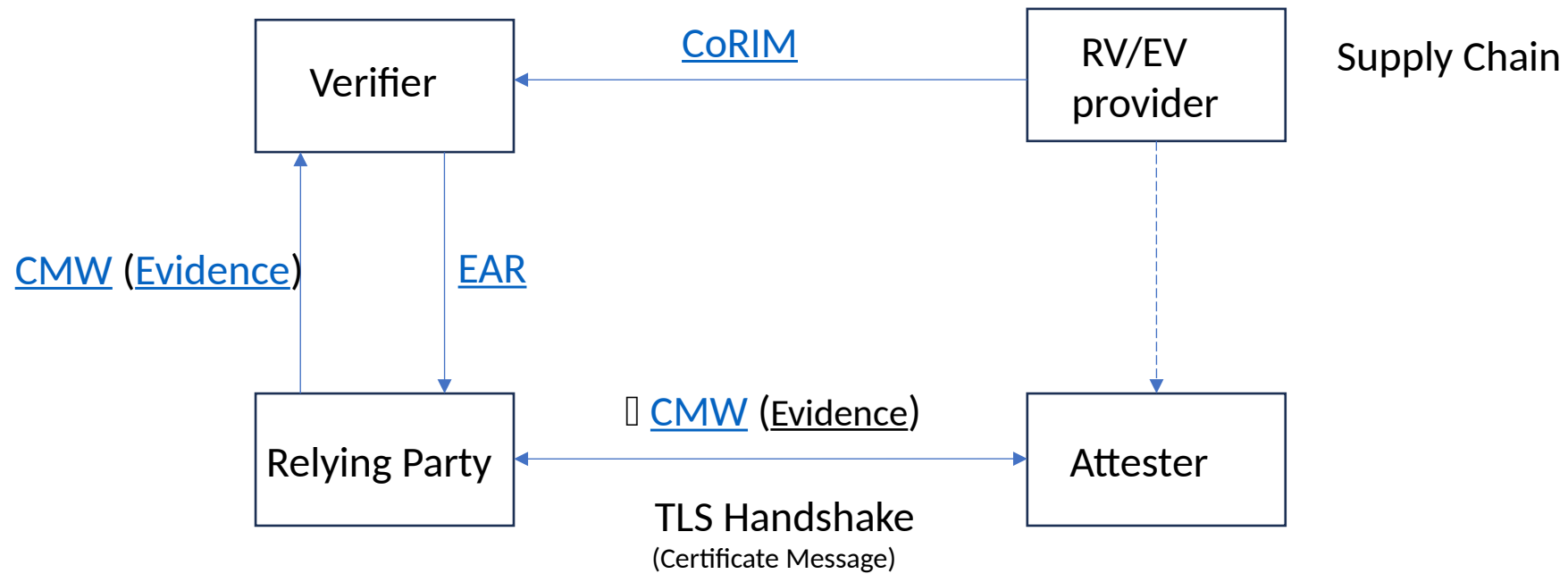
Message Flow



Message Flow



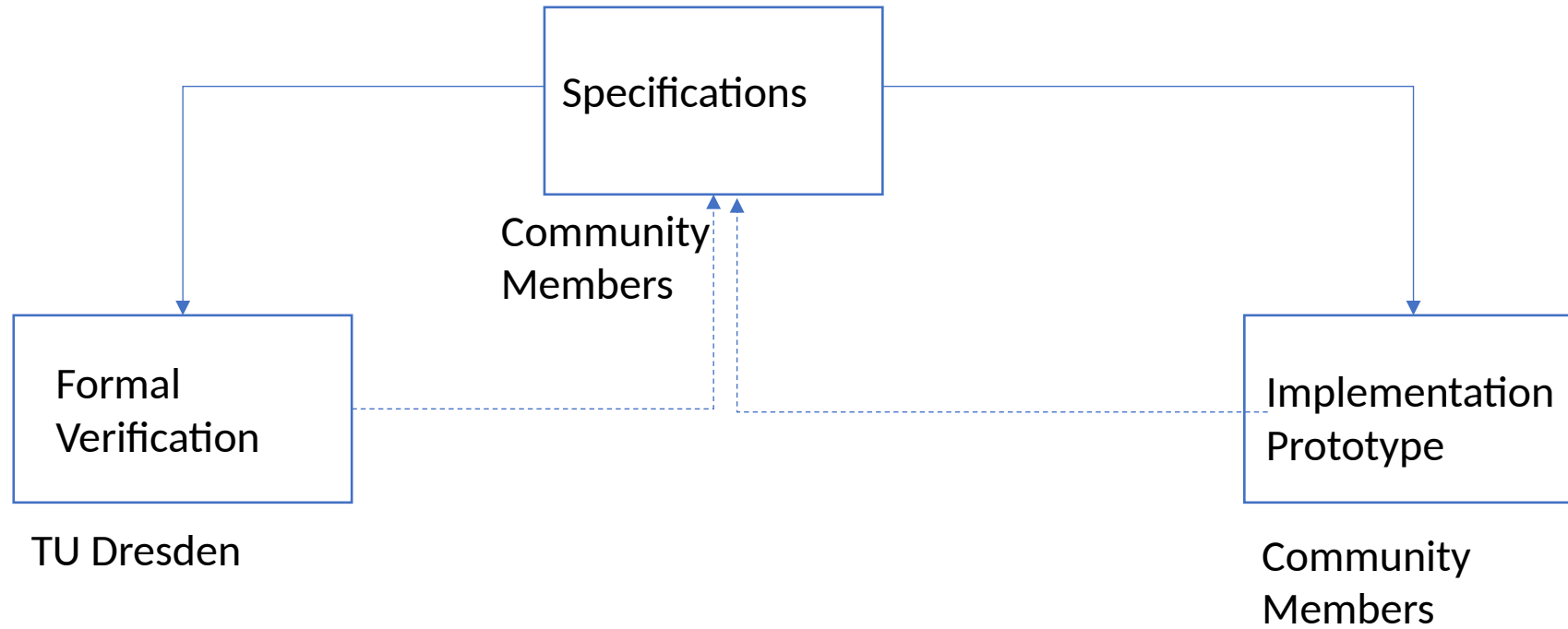
Mapping to RATS



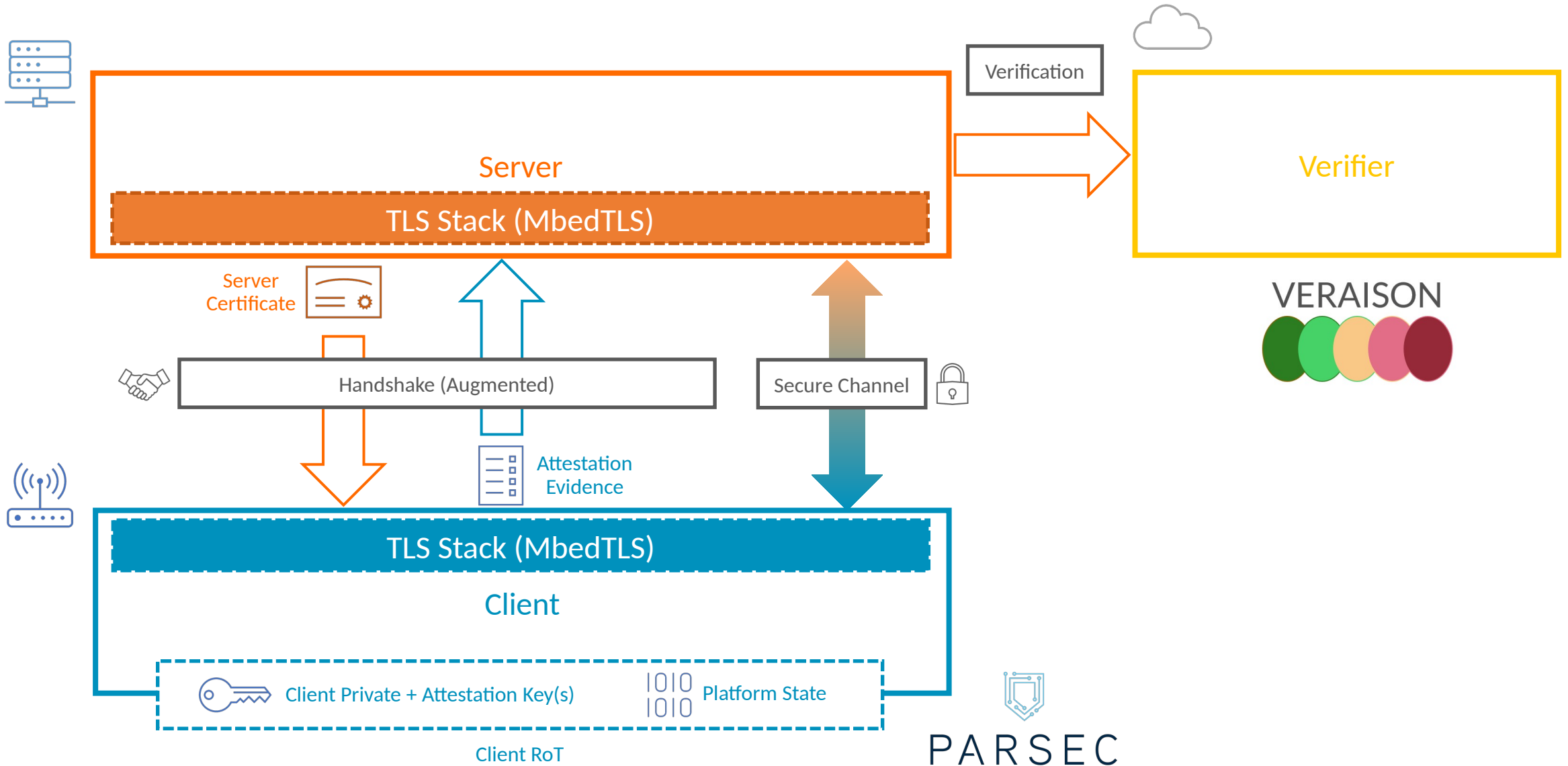
Usage of RATS Draft

Draft Name	Describes
Attestation in TLS and DTLS	Describes TLS extensions to use attestation for authentication
EAT based Key attestation Token	Evidence format of combined key and platform attestation
CoRIM	Concise Reference Integrity Manifest (CoRIM), a standardised way to convey Reference Values and Endorsed Values to a Verifier
EAT Attestation Results (EAR)	An EAT profile for conveyance of Attestation Results
CMW	A format used to Wrap RATS Messages in a protocol agnostic way
EAT Collection Types	An extension to EAT allowing the top-level token to consist of a collection of otherwise defined tokens

Current Activities & Collaborations



Prototype Architecture



Main Open-Source Repositories

Repository Name(link)	Contains
CCC Attested TLS PoC	Central space for open collaboration on the proof of concept
Parsec	Library to abstract Attester Evidence Formats
Mbed TLS library	TLS Library
Veraison	Attestation Verification deployment
ctoken	A C library to implement EAT, CWT and UCCS
t_cose	A C Library to implement COSE RFC 9052

Status of Implementation

- An end-to-end working proof of concept is now available
 - From Attester through a TLS implementation, to a Verifier
 - Uses Background check model, with TPM 2.0 as a RoT
- Open-Source availability of entire stack
 - The components themselves are open-source software
 - Project harbored under CCC-Attestation SIG
- Work In Progress on a Confidential Computing (CC) version of Attester running in a confidential environment (ARM-CCA) and performing an end-to-end Attested TLS handshake between Client (Attester), Server (RP) and a Verifier
- Community Members Welcome to engage in implementation to bring in other attestation formats

Future Work

- To enhance draft to include RATS passport model
- Implement a PoC based on the passport model